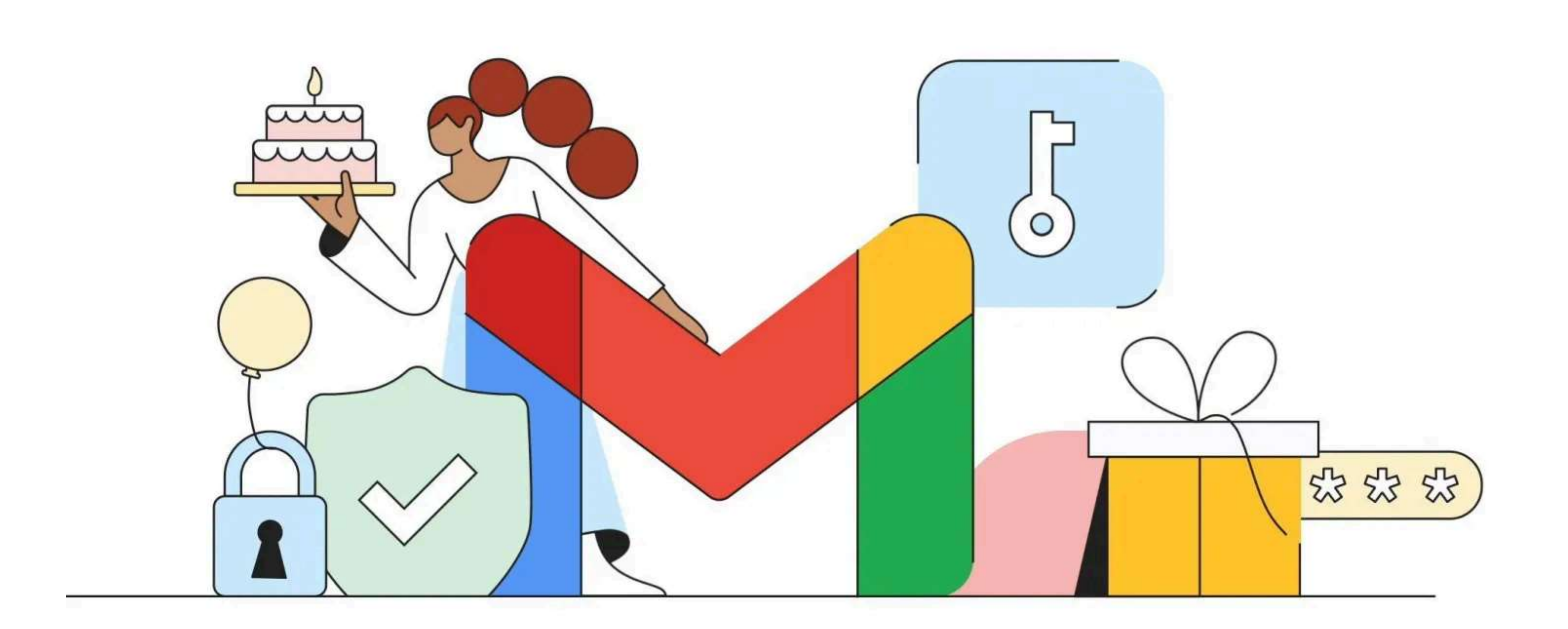
تكنولوجيا

«غوغل» تطرح التشفير التام للرسائل الإلكترونية للأعمال عبر «جيميل» بهدف حماية البيانات المؤسسية



في المرحلة الأولى يقتصر التشفير على الرسائل داخل نفس المؤسسة على أن يتم توسيعه لاحقاً ليشمل جميع العملاء والبريد الإلكتروني الخارجي (غوغل)

لندن: نسيم رمضان

نُشر: 18:00-2 أبريل 2025 م . 04 شوّال 1446 هـ

في خطوة بارزة لتعزيز الخصوصية وتبسيط أمان البريد الإلكتروني للمؤسسات، أعلنت شركة «غوغل» عن طريقة جديدة ومبسطة لإرسال الرسائل الإلكترونية المشفّرة تشفيراً تاماً (E2EE) عبر «جيميل» (Gmail). وتستند هذه الميزة إلى بروتوكول «S/MIME» وهو اختصار لـ«توسعة البريد المتعدد الأغراض الآمن». الهدف هو جعل الاتصالات المشفرة أكثر سهولة، حتى للجهات التي لا تمتلك بنية تحتية تقنية متقدمة.

وفي منشور رسمي على مدونة «Google Workspace»، كشفت الشركة أن الميزة الجديدة بدأت في الوصول إلى عدد محدود من مستخدمي الأعمال ضمن إصدار تجريبي (بيتا). وتهدف هذه المبادرة إلى تقليل التعقيد المرتبط عادةً بتشفير البريد الإلكتروني، مما يتيح للمؤسسات من جميع الأحجام حماية مراسلاتها الحساسة بسهولة ودون الحاجة إلى موارد تقنية كبيرة.

تجربة تشفير سلسة

بعكس الطرق التقليدية التي تتطلب إعدادات معقدة أو دعماً تقنياً متخصصاً، تعتمد «غوغل» نهجاً يركز على البساطة. سيتمكن المستخدمون من إرسال رسائل إلكترونية مشفرة إلى الزملاء ضمن نفس المؤسسة بخطوات قليلة فقط. وتُشفّر هذه الرسائل باستخدام مفاتيح يتم التحكم بها من قبل المستخدمين أنفسهم، دون أن يكون لـ«غوغل» إمكانية الوصول إليها، مما يضمن خصوصية تامة للبيانات. وأكدت «غوغل» على أهمية هذا الجانب في إعلانها قائلة: «لقد أحرزنا تقدماً مهماً في تمكين المؤسسات من جميع الأحجام من الاستفادة من اتصالات بريد إلكتروني آمنة»، وذكرت «غوغل» أن هدفها هو جعل التشفير التام سهلاً وفعالاً ومتاحاً على نطاق واسع.

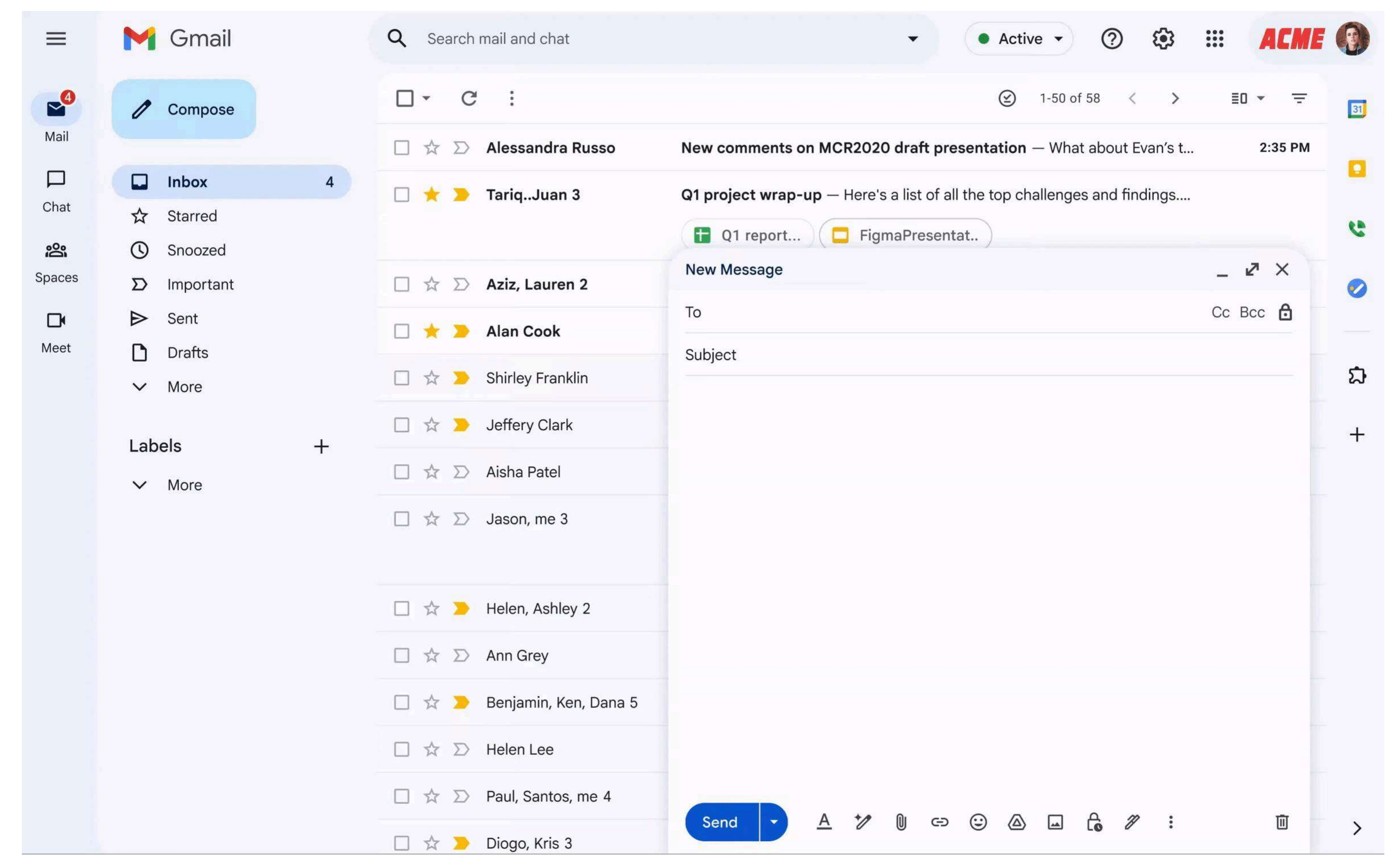
كيف تعمل الميزة؟

بالنسبة للشركات المشتركة في خدمة «Google Workspace» أصبح إرسال بريد إلكتروني مشفر الآن بسيطاً مثل:

1- كتابة الرسالة في «جيميل»- اختيار خيار التشفير قبل النقر على إرسال

إذا كان المستقبل أيضاً من مستخدمي «جيميل»، فسيتم فك تشفير الرسالة تلقائياً عند الوصول.

أما إذا كان المستقبل يستخدم خدمة بريد إلكتروني مختلفة (مثل «أوتلوك» Outlook أو «ياهو» Yahoo)، فسيحصل على دعوة لعرض الرسالة بشكل آمن عبر حساب ضيف في « Google Workspace»، مما يحافظ على التشفير حتى خارج نظام «غوغل».



يتم التحكم بمفاتيح التشفير من قبل المستخدمين أنفسهم ما يعني أن «غوغل» لا يمكنها الوصول إلى محتوى الرسائل (غوغل)

ما بعد «جيميل»

في المرحلة الأولى، ستقتصر ميزة التشفير التام على مستخدمي «جيميل» (Gmail) ضمن نفس المؤسسة. ولكن خلال الأسابيع القادمة، تخطط «غوغل» لتوسيع الميزة لتشمل إمكانية إرسال رسائل مشفّرة إلى مستخدمين على منصات بريد إلكتروني أخرى. وحتى بالنسبة للمستلمين غير المستخدمين لـ«Gmail»، لم تهمل «غوغل» تجربة الاستخدام. فهؤلاء المستخدمون سيتلقون دعوة لعرض الرسالة المشفّرة عبر بيئة آمنة ومقيّدة تتيح لهم الوصول إلى البريد دون المساس بالأمان.

مجموعة جديدة من ميزات الأمان

إلى جانب ميزة التشفير التام، تضيف «غوغل» عدداً من الأدوات الأمنية الجديدة إلى «جيميل» لتعزيز حماية بيانات الأعمال منها الوضع الافتراضي لـ«CSE»، حيث يمكن لمسؤولي تكنولوجيا المعلومات الآن تعيين التشفير التام كإعداد افتراضي لجميع الرسائل. أيضا ميزة تسميات التصنيف التي تساعد هذه التسميات المستخدمين على تحديد مستوى حساسية محتوى الرسائل الإلكترونية. أداة منع فقدان

البيانات (DLP) التي تتيح هذه الأداة تطبيق تسميات وسياسات حماية تلقائياً استناداً إلى محتوى الرسالة. تُظهر هذه التحديثات التزام «غوغل» بتوفير أدوات أمان قوية تمنح المؤسسات مزيداً من السيطرة على بياناتها، وتخلق بيئة عمل رقمية أكثر أماناً.

خطوة نحو مستقبل أكثر خصوصية

تعكس هذه الخطوة توجه «غوغل» نحو دمج الأمان مع سهولة الاستخدام، من خلال توفير وسائل حماية متقدمة لا تتطلب معرفة تقنية متخصصة. ورغم أن التشفير يُعد ممارسة أساسية لحماية البيانات، فإن تعقيد تنفيذه كان عائقاً كبيراً في السابق. ويبدو أن تحديث «جيميل» الأخير يوازن بين القوة والسهولة. وتعتزم «غوغل» جمع ملاحظات المستخدمين خلال فترة الإصدار التجريبي، قبل الإطلاق الكامل.

